IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF A BLACK IPHONE LOCATED IN AN EVIDENCE LOCKER IN WEST VALLEY CITY, UTAH, AS MORE PARTICULARLY DESCRIBED IN ATTACHMENT A	Case No. 2:24-mj-00682 DBP

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Zackary T. Rhinehart, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations ("HSI"). I have been employed by HSI since July 2017. Prior to HSI, I was a Police Officer, Criminal Investigator, and FBI Task Force Officer in Cameron County, Texas for a combined eight years. As an HSI Special Agent, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 21 and Title 18 of the United States Code. In my work with HSI and from my previous experience, I have received training and conducted investigations that involve various offenses to include fraud, theft, drug trafficking, and money laundering. I have received courses of instruction relating to investigative techniques and financial investigations. In addition, I have

conducted follow-up investigations concerning the concealment of illegal proceeds, assets, bank records, etc., and the identification of co-conspirators through the use of ledgers, records, telephone bills, and photographs, as related to financial crimes and drug trafficking. I have authored multiple state and federal search warrants to include pen register, trap and trace devices, and Title III (wiretap) affidavits. I have also assisted, conducted, and led multiple bank fraud investigations involving multiple subjects, across state lines, resulting in federal charges and convictions.

3. Among other duties, I am leading the federal investigation into the **Matthew ACQUAH** bank fraud ring ("BFR") that is alleged to be involved in the use of counterfeit identification documents to fraudulently open bank accounts and obtain cash advances on lines of credit under the names of unwitting victims.[1] This BFR is documented as operating in Utah, Nevada, Idaho, California, and elsewhere.

4. The following is based on conversations with HSI Salt Lake City ("SLC") case agents, and oral and written reports provided by the SLC Office. Since this affidavit is being submitted for a limited purpose, I have not included every fact I know about this investigation. I set forth only facts necessary to establish the foundation for the requested Order.

5. Based on the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe violations of federal law have been committed by ACQUAH, **Jordan BATTLE**, **Jamari CHAPMAN**, **Emas HAMA**, **Lucky HATHAWAY**, and others known and yet unknown, including: 18 U.S.C. §§ 1344, 1349, Bank Fraud and Conspiracy to Commit Bank Fraud; and 18 U.S.C. § 1028A, Aggravated Identity Fraud (hereinafter referred to as the

[1] I will be transitioning the lead investigative role to Special Agent Christopher Snow as I start a new HSI assignment at the end of the month.

"TARGET OFFENSES"). There is also probable cause to search the Device, further described below and in Attachment A, for the things described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The item to be searched is a black iPhone, which was seized from HATHAWAY on June 20, 2024, hereinafter the "Device." The Device is currently in HSI's possession at 2975 S. Decker Lake Drive, West Valley City, Utah, 84119.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. In March 2024, the Taylorsville Police Department notified HSI-SLC of a bank fraud ring operating in multiple states, including Utah. Reports indicated that various individuals were opening bank accounts with stolen identities to obtain lines of credit at Utah-based credit unions, and then drawing thousands of dollars on those unauthorized lines of credit. The perpetrators were observed by tellers and video surveillance using cell phones during the unauthorized transactions. A preliminary investigation identified actual losses for Utah banks in an amount exceeding $450,000, with more losses attributed to affiliated BFRs.

9. In March 2024, HSI and the Taylorsville Police Department interviewed a cooperating defendant ("CD") who was in custody in the SLC area for state fraud-related charges. During the interview, the CD waived his/her rights and agreed to speak with investigators. The CD explained that he/she was recruited by a subject the CD knew as "Matt" or "Playboy Prince," which is ACQUAH's Instagram handle. The CD explained that he/she was provided multiple stolen identities by ACQUAH who instructed him/her on how to fraudulently open a line of credit and cash advance using the stolen identities, generally through text message

or encrypted messaging applications. The CD admitted conducting several successful fraudulent transactions in and around the SLC area, all while maintaining contact with ACQUAH or other handlers through text message or encrypted messaging applications. Investigators confirmed through banking documents and surveillance photos that the CD did as stated, successfully obtaining over $70,000 in cash from Utah credit unions using the stolen identities. The CD further identified HAMA and HATHAWAY as ACQUAH's co-conspirators and explained that they acted as drivers and handlers during a fraud spree in the SLC area in January 2024.

10. Investigators obtained a search warrant for ACQUAH's iCloud account which showed ACQUAH was heavily involved in fraud and further corroborated the CD's account. He had hundreds (estimated) of photos reflecting third parties' personal identifying information ("PII"), bank account information, and pictures of numerous counterfeit U.S. passport cards, drivers' licenses, and various other fraudulent identification documents.

11. In October 2023, ACQUAH sent a series of lengthy messages to a large iMessage group chat with over 17 recipients, detailing "[t]he profitability of a hot dog stand," with recommendations to "[c]onsider seeking advice from a local business advisor to help [] develop a more accurate business plan." Among the recipients of ACQUAH's cryptic messages were "avolvestudios@gmail.com" and "braianstiwar2@hotmail.com"—some of his "lid plugs" or ID fabricators—as well as at least two known conductors, HATHAWAY and an unindicted co-conspirator. HATHAWAY and the unindicted co-conspirator were arrested together in November 2023 following a high-speed vehicle chase in Millard County, and later released. The group chat contains numerous deleted messages and admonishments to "check Telegram" or "[d]elete . . . messages." The same group chat was later used to coordinate logistics for "plays," profit sharing arrangements, money transfers, and encrypted communications.

12. From the iCloud data, investigators learned that ACQUAH communicated with HATHAWAY using text messages and encrypted messaging applications. HATHAWAY was identified based on the phone subscriber information for his phone number, as well as the transmission of photographs containing his likeness. Text messages extracted from ACQUAH's iCloud included conversations between ACQUAH and HATHAWAY coordinating the January 2024 fraud spree and negotiating compensation for HAMA's role during the same fraud spree. ACQUAH's iCloud account also contained photographs of HATHAWAY posing with large stacks of U.S. currency at the same time the January 2024 fraud spree was underway.

13. ACQUAH's iCloud data and the CD's phone also contained group text messages and encrypted messages between ACQUAH, HATHAWAY, HAMA, and others, coordinating fraud activities and the logistics for their January 2024 fraud spree.

14. Additionally, ACQUAH's iCloud account contained communications with fraudulent identification documents for BATTLE and CHAPMAN. In BATTLE's case, text messages show efforts by ACQUAH, HATHAWAY, and BATTLE to arrange future fraud sprees in Utah using BATTLE's girlfriend to conduct the unauthorized transactions. Specifically, ACQUAH, HATHAWAY, and BATTLE used text messages to discuss money transfers, relay victim information, and facilitate travel for fraud sprees. BATTLE was identified based on the phone subscriber information for his phone number. Based on the foregoing, law enforcement officers tracked BATTLE's girlfriend's vehicle, which was driven to Utah. Surveillance of the vehicle confirmed it was driven by BATTLE during this trip, which coincided with a known fraud spree perpetrated by BATTLE's girlfriend. During a second fraud spree in May 2024, BATTLE made a hotel reservation in the SLC area (using his real name) and was captured on the hotel's surveillance system with the perpetrator of numerous unauthorized

transactions during the same week. Further, call records from BATTLE's phone number show extensive communications with other known co-conspirators during fraud sprees/attempts by the ACQUAH BFR in mid-2024. Given the CD's explanation of the fraud scheme, which relies on constant communication between the perpetrator and handler, it is believed BATTLE used a cell phone to communicate with co-conspirators during their unauthorized transactions.

15. ACQUAH's iCloud account further contained PII for individuals later victimized by CHAPMAN, as well as fraudulent identification documents for these victims which bore photographs of CHAPMAN's likeness. Based on the foregoing, law enforcement officers tracked CHAPMAN's vehicle, which was observed driving to meetings with known co-conspirators during fraud sprees/attempts by the ACQUAH BFR in mid-2024. Video surveillance from credit unions show CHAPMAN using fraudulent identification documents to make unauthorized transactions, while often referencing his cell phone, which is consistent with the CD's description of the fraud scheme.

16. Investigators have identified over 20 subjects that are part of the ACQUAH BFR. Investigators have bank documents that show the fraud has continued and even increased after the arrest of the CD in January 2024. Investigators have bank documents and information from the iCloud warrant that show the ACQUAH BFR attempted the bank fraud in Utah as recently as May 8, 2024.

17. On June 5, 2024, ACQUAH, BATTLE, CHAPMAN, HAMA, and HATHAWAY were indicted by a federal grand jury in the District of Utah for the TARGET OFFENSES in case number 2:24-cr-00190-RJS. Arrest warrants were issued for their arrest.

18. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know that the Device is capable of and

frequently used to communicate with other individuals, take and store photographs and videos, and used for internet searches, among other things. Examining data stored on Device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device (and sometimes by implication who did not), as well as evidence relating to the commission of the offenses under investigation. For example, in my training and experience, individuals involved in identity theft or bank fraud frequently communicate with co-conspirators using electronic devices to discuss strategy, obtain information about identity theft victims, and relay fraudulent account information.

19. The Device is currently in the lawful possession of HSI. It came into the HSI's possession after it was seized incident to HATHAWAY's arrest on or about June 20, 2024, pursuant to the aforementioned arrest warrant.

20. The Device is currently in storage at 2975 S. Decker Lake Drive, West Valley City, Utah, 84119. In my training and experience, I know the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call

log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media.

Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data

and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address

so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

27. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Zackary Rhinehart
ZACKARY RHINEHART
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on July 9, 2024:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The item to be searched is a black iPhone, which was seized from HATHAWAY on June 20, 2024, hereinafter the "Device." The Device is currently in HSI's possession at 2975 S. Decker Lake Drive, West Valley City, Utah, 84119.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 1344 (Bank Fraud), 1349 (Conspiracy to Commit Bank Fraud), and 1028A (Aggravated Identity Theft) and involve HATHAWAY since November 2023, including without limitation records pertaining to the following:

   a. identifying information of identity theft victims;

   b. information regarding credit union or bank branch locations as well as dates, places, and amounts of specific transactions involving HATHAWAY;

   c. any information related to identity theft or forgeries;

   d. any information related to sources of forged documents or victims' identities (including names, addresses, phone numbers, or any other identifying information), including communications therewith;

   e. any information recording HATHAWAY's schedule or travel from Decmber 2023 to the present, including correspondence or other information regarding travel, rental cars, hotels, and related arrangements; and

   f. all bank records, checks, credit card bills, account information, and other financial records;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of the attachment to the Device of other storage device or similar containers for electronic evidence;

4. Evidence of the times the Device was used;

5. Passwords, encryption keys, and other access Device that may be necessary to access the Device;

6. Records of or information about Internet Protocol addresses used by the Device; and

7. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.